**Université de Nantes – 2010 – 2011**

# Rapport de Stage

Mise en place d'un serveur de supervision

Licence 3 Informatique

Quentin GAUTIER

Responsable de stage : Abdelouahab MEKAOUCHE
Maitre de Stage : Sébastien BURGAUD

Avril – Juin 2011

## *Remerciement*

*Je remercie d'abord Mr Le Biez (Président Directeur Général) pour m'avoir accueilli durant les neuf semaines de stage au sein du groupe SOFIA.*

*Je tiens particulièrement à remercier Mr Burgaud pour m'avoir accueilli comme un membre à part entière de son service et pour m'avoir accordé sa confiance sur le projet à mener.*

*Mes remerciements aux membres des autres services du groupe SOFIA que j'ai côtoyé quotidiennement et dont j'ai apprécié la gentillesse et la bonne humeur.*

*Je remercie également mon tuteur de stage, Mr Mekaouche pour ses conseils avisés.*

# Résumé

Rapport de stage de fin d'études de troisième année de licence Informatique qui s'est déroulé du 18 avril 2011 au 17 juin 2011 au sein de la holding SOFIA.

**Thème** : Mise en place d'un serveur de supervision d'un parc informatique.

Ce rapport porte sur la mission de la création d'un serveur de supervision. Le serveur sera utilisé par l'informaticien de SOFIA afin de surveiller son réseau informatique qui est étalé géographiquement sur une large zone. Ce rapport évoque les conditions d'étude, de mise en place et de configuration de la solution de supervision.

Un bilan clôture ce document et synthétise l'expérience et le ressenti durant ces 9 semaines de stage.

En annexe, des exemples de code de configuration, des captures d'écran, le fichier regroupant la liste des machines à superviser et le manuel d'utilisateur à disposition du superviseur et des personnes susceptible d'utiliser la supervision.

## Abstract

Internship report of end study third year on computer sciences license. It’s which took place from April 18th, 2011 to June 17th, 2011 in the SOFIA holding company.

**Subject**: Establishment of a monitoring server from computer equipment.

This report focuses on the mission of creating a monitoring server. This server will be used by the SOFIA's computer scientist. With it, he will be allowed to watching his network which's spread geographically. This report discusses the conditions of establishment, studying and configuration of this server.

A summary concludes this document and summarizes the experience gained and felt during these 9 weeks of training.

In annex, the Nagios’s code source of configuration system, screenshots, the file with data of the network, and the user's book for using the application in this type of configuration.

# Sommaire

*Remerciement* ..... 2
Résumé ..... 3
Abstract ..... 4

1 Le groupe SOFIA et la filiale Clin d'œil ..... 7
1.1 SOFIA : Fiche d'identité ..... 7
1.2 SOFIA : Son histoire ..... 8
1.3 SOFIA : Son organisation ..... 9
1.4 Présentation de son réseau Informatique ..... 10

2 Introduction ..... 11
2.1 Le cadre ..... 11
2.2 La Description de la tâche confiée ..... 11
2.3 La répartition du travail ..... 12

3. Prétraitement ..... 13
3.1 Travail de recherche ..... 13
3.1.1 Solutions de monitoring payantes ou gratuites ..... 13
3.1.2 Comparaison des solutions gratuites retenues. ..... 14

4. Fonctionnement de Nagios et d'EyesOfNetwork ..... 19

5. Installation et Configuration ..... 20
5.1 Eléments à superviser et installation du serveur ..... 20
5.2 Configuration des machines clientes ..... 20
5.2.1 Explications ..... 20
5.2.2 Installation par automatisation ..... 21
5.2.3 Installation par télémaintenance ..... 22
5.2.4 Installation manuelle via logiciel de contrôle à distance. ..... 22
5.3 Configuration de l'AS/400 ..... 23
5.4 Récupération de l'état de services sur les serveurs SOFIA ..... 25
5.5 Configuration des Templates ..... 25

6. Finalisation du projet ..... 27
6.1 Tests et ajustements ..... 27
6.2 Gestion des imprévus et problèmes récurrents ..... 27

7. L'application Web ..... 29
7.1 Description de la tâche ..... 29
7.2 Contexte ..... 29
7.3 Solutions apportées ..... 30

Synthèse du stage ..... 31

Webographie ..... 32

Bibliographie ..... 32

Annexes ..... 33
I - Exemple de fichiers configuration de Nagios ..... 33
II - Exemple de mail envoyé automatiquement par Nagios en cas de pannes ..... 35
III - Liste Supervision avec services à traiter ..... 36
IV - Captures d'images de la supervision Nagios ..... 37
1.Affichage d'un serveur et de l'état de ses services. ..... 37
2.Affichage de la cartographie automatique de Nagios ..... 38
3. Affichage d'une courbe fonction du temps de l'état d'une machine ..... 39
V - Manuel d'utilisateur (procédure) ..... 40

# 1 Le groupe SOFIA et la filiale Clin d'œil

## 1.1 SOFIA : Fiche d'identité

| |
|---|
| Raison Sociale: |
| Société Financière Atlantic |
| Statut juridique: |
| Société Anonyme à Directoire et Conseil de surveillance<br>au capital de 3 125 000 € |
| Code APE |
| 741 J: Administration de sociétés |
| Date de création: |
| 1990 = création de SOFIA<br>1961 = création de la société Atlantic Distribution |
| Adresse: |
| 2 rue Georges Clémenceau<br>44612 SAINT-NAZAIRE |
| Effectif: |
| Société mère = 25<br>Groupe = 1007 (751 CDI ) |
| Chiffres clés : |
| Résultat d'exploitation 2009= 4 230 902 €<br>Bénéfice exercice 2009 = 3 727 511 €<br>Résultat consolidé 2009 = 2 267 798 €<br><br>C.A. consolidé 2009= 104 422 000 €<br>C.A. consolidé 2008 = 98 919 000 €<br>Taux de croissance = + 5, 6 %<br><br>Capitaux Propres consolidés 2009 = 22 164 185 €<br>Capitaux propres consolidés 2008 = 21 022 786 €<br><br>Total Bilan consolidé 2009 = 78 552 336 €<br>Total Bilan consolidé 2008 = 87 057 966 € |

## 1.2 SOFIA : Son histoire

| | |
|---|---|
| 1961 | Création de la société Atlantic Distribution<br>Distribution de fioul domestique<br>Secteur très localisé autour de Saint-Nazaire |
| 1970 | Développement des activités : négoce de robinetterie industrielle<br>Distribution des marques Butagaz et Camping Gaz |
| 1973 | Création du premier magasin de bricolage<br>Franchise à l'enseigne OBI |
| 1978 | Création du premier magasin de jardinage<br>Franchise à l'enseigne JARDILAND |
| 1982 à 1988 | Stratégie de croissance interne, investissements très importants<br>Extension des secteurs d'activités<br>Création de la SAS Loire Entrepôts Transports (1985) |
| 1990 | Filialisation des activités<br>Atlantic Distribution devient la société holding SOFIA |
| 1994 à 1995 | Acquisition et développement du groupe des sociétés CLIN D'ŒIL<br>Activité de commerce de parfumerie (6 parfumeries à fin 95) |
| 1998 | Ouverture du premier magasin sous l'enseigne Elytis (Nantes) |
| 2005-2006 | 40 parfumeries franchisées ou labellisées Elytis en France, de Cherbourg à Lourdes<br><br>Nouveau contrat de franchisage<br>Magasins de Bricoland passent sous l'enseigne Leroy Merlin |
| 2010 | 50 parfumeries franchisées ou labellisées Douglas en France, de Cherbourg à Biarritz |

## 1.3 SOFIA : Son organisation

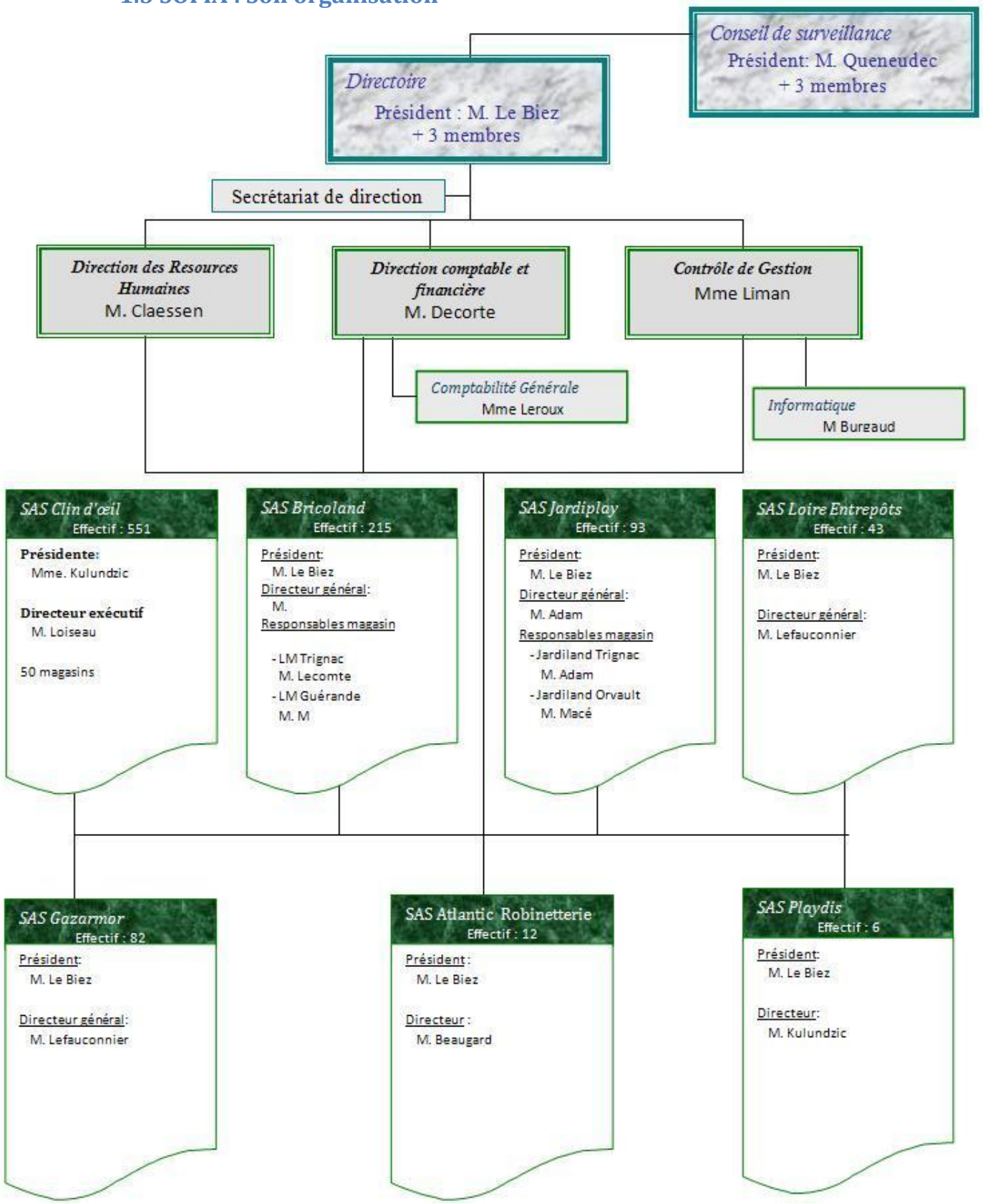



Figure1 : Organisation du groupe SOFIA

## 1.4 Présentation de son réseau Informatique

Nous ne parlerons ici que du réseau informatique dont il sera question dans ce rapport. Il sera exclu toutes machines ou serveurs qui ne font pas partie intégrante du sujet de stage.

Le réseau informatique chez SOFIA est  distribué sur plusieurs points géographiques. Tout d'abord le siège à Saint-Nazaire, on y trouve un certain nombre de postes de travail mais surtout la plupart des serveurs de l'entreprise. Ils ont tous été virtualisé[1] dans le courant du mois de Juin pour ne laisser qu'un serveur AS/400.

Toujours à Saint-Nazaire, la SAS Clin d'œil dispose de son propre bâtiment et donc de son propre sous-réseau avec deux serveurs. La firme s'occupe aussi entre autre de magasins franchisé Douglas. Chaque magasin est équipé d'un routeur, d'au moins un ordinateur allumé 24h/24 pour laisser des opérations s'exécuter la nuit.

Enfin les filiales SAS Playdis et SAS Loire Entrepot, en plus d'avoir certaines machines ont chacune d'elle un serveur fonctionnant sous Windows Server.

[1] Virtualisation : consiste à faire fonctionner sur un seul ordinateur plusieurs systèmes d'exploitation comme s'ils fonctionnaient sur plusieurs ordinateurs

# 2 Introduction

## 2.1 Le cadre

Le stage s'est déroulé du 18 avril 2011, au 17 juin 2011 pour un total de neuf semaines de stage au sein du groupe SOFIA. Dans un souci d'optimisation de la gestion de son réseau informatique, le groupe SOFIA a mis en place ce stage pour la création d'un serveur de supervision. Le travail a été effectué sur une machine sous Windows XP ayant accès via des logiciels tel que VNC[2] permettant un contrôle à distance des différents serveurs et ordinateurs à configurer. Le serveur de supervision lui était accessible via un logiciel VMWare.

## 2.2 La Description de la tâche confiée

Le stage s'est déroulé via deux tâches distinctes. La principale et celle qui a fait l'objet de la grande majorité du temps passé durant ce stage concerne la mise en place d'une supervision et la seconde tâche à consister à reprendre, corriger et compléter une application web de l'intranet SOFIA.

Tout d'abords, il faut définir la supervision. La supervision ou « monitoring » est une activité de surveillance en continue d'un parc informatique. Un serveur de supervision contrôle en permanence l'état de chaque serveur, routeur et appareil relié à un réseau. Il est possible de relever et mesurer un grand nombre de données qui sont traitées par le serveur pour permettre une surveillance en temps réel d'un grand nombre de machines et de leur service.

Dans l'optique de surveiller un parc informatique dispersé géographiquement, la tâche qui m'a été confié était de mettre en place un serveur de supervision après avoir étudié les différentes solutions proposée dans ce domaine, ainsi que de configurer ce serveur pour surveiller des éléments précis du parc informatique de la société SOFIA. En effet, des

[2] VNC : Virtual Network Computing est un logiciel d'accès à un bureau distant retransmettant saisies clavier et souris sur cette machine distante.

magasins franchisés, dont le groupe a la direction, se situe à plusieurs endroits sur tout l'ouest de la France. Chaque magasin constitue un sous réseaux qu'il faut superviser.

Un supplément dans ma tâche de stagiaire en informatique m'a été proposé en plus de la mise en place du serveur de monitoring. Il s'agit l'amélioration et la correction d'une application web développé avec le langage PHP[3].

## 2.3 La répartition du travail

Dans un premier temps, il m'a été demandé de faire des recherches sur toutes les solutions de monitoring. Comparer les offres payantes et gratuites et trouver l'offre la plus adaptées aux besoins de l'entreprise. Il a ensuite fallu mettre en place la solution adoptée en l'installant sur une machine virtuelle de l'entreprise.

Dans un second temps, il a fallu configurer l'ensemble du réseau à superviser ainsi que le serveur en lui même pour qu'il puise récolter les informations voulues. Enfin, des ajustements au niveau de la configuration du serveur permettront d'avoir le juste équilibre dans la surveillance du réseau.

[3] PHP : Langage de scripts utilisés pour le développement d'application Web dynamiques

# 3. Prétraitement

## 3.1 Travail de recherche

Avant de mettre en place un quelconque serveur de supervision, il a fallu exercer un travail de recherche sur la multitude de solutions existantes pouvant répondre au problème de l'entreprise. Chaque solution ayant des avantages et des inconvénients que nous décrirons dans cette partie.

### 3.1.1 Solutions de monitoring payantes ou gratuites

Il existe deux grands types de solutions de monitoring, d'un côté les solutions payantes :

- HP OpenView
- What'up Gold
- Dell OpenManage
- Microsoft Operating Manager

Et on a aussi des solutions gratuites :

- Nagios
- Zabbix
- Shinken
- FAN 2.1 (Fully Automated Nagios)
- EyesOfNetwork
- Multi Router Traffic Grapher
- Xymon

Beaucoup des solutions gratuites sont basées sur la solution Nagios. Et devant la multitude de solutions gratuites et sous licence libre, les solutions payantes ont rapidement été mises de côté. La taille du réseau à superviser, et l'informaticien de SOFIA étant seul,

il n'est pas utile de mettre en place un service payant bien plus optimisé pour les réseaux importants ou les entreprises de plus grande taille. De plus, l'argument d'une solution gratuite est bien entendu de poids puisqu'il permet à l'entreprise de ne pas engager de frais supplémentaires pour la supervision de son parc informatique. Le désavantage de laisser de côté cette solution est de se priver d'un soutien technique des entreprises proposant une solution payante. Souvent vendu de cette façon, les logiciels payants ont en effet un soutien technique performant permettant de mettre en place sur un réseau informatique, une solution de monitoring facilement et rapidement.

Les solutions gratuites proposent un large choix de fonctionnalités pour répondre à tous les besoin en monitoring de l'entreprise. Cependant, il n'est pas facile de faire le tri dans tous ces logiciels, c'est ce que nous allons pourtant faire dans le prochain point.

### 3.1.2 Comparaison des solutions gratuites retenues.

Après de multiples recherches sur des forums spécialisés français et étrangers, nous avons retenu cinq solutions qui revenaient le plus souvent. En effet, le problème de choisir un logiciel de monitoring pour des parcs informatique d'une centaine de machines est récurrent, et les solutions proposées sont souvent les mêmes. Nous allons voir en détail donc les différentes solutions proposées.

#### *3.1.2.1 Nagios/Centreon*

Avec le logiciel Centreon, Nagios est la solution gratuite de monitoring la plus répandue, c'est aussi autour de ce logiciel que la communauté d'utilisateurs est la plus grande ce qui lui apporte un avantage certains. En effet, on trouvera souvent une réponse à un problème auprès de cette communauté. Complètement open source, le logiciel est très complet car il peut s'enrichir de plugins[4] qui peuvent être programmés dans n'importe quel langage tant que des règles d'entrées et sorties sont respectées. Cela apporte une très grande souplesse au logiciel car les plugins restent compatibles avec Nagios même si celui-ci se met à jour. Le logiciel Centreon qui se base sur

[4] Plugins : module d'extension qui complète un logiciel

Nagios sert d'interface, bien qu'utilisable seul. La configuration de Nagios se faisant manuellement dans des fichiers de configuration, Centreon sert à rendre le tout bien plus convivial via une interface simple et complète. Aussi compatible avec Cacti, un logiciel de supervision qui permet l'affichage sous forme de graphique, Nagios est un outil extrêmement complet. Enfin, en plus d'une communauté très importante, il existe une documentation très complète sur ce logiciel.

Basé sur une base de données de type RR[5] la base de données a une taille fixe. En effet, Nagios stocke les informations récoltées sur le réseau afin de pouvoir afficher des graphiques de tendances et des historiques. Plus le volume d'information à sonder sur un réseau volumineux sera important, plus il faudra penser à créer une base de données suffisamment importante cas la taille sera fixée et un mauvais choix limitera les fonctionnalités de Nagios. La taille fixe permet cependant de contrôlé l'espace disque du serveur de supervision.

Nagios a de nombreuses qualités, mais il y a quelques inconvénients qui peuvent nous faire choisir un autre logiciel à sa place. Décrit comme difficile à prendre en main, sa courbe d'apprentissage est plutôt longue, c'est-à-dire qu'il faut un nombre d'heures non négligeables avant de comprendre les subtilités du logiciel. Il en est de même pour son installation. Les mise à jours, bien qu'optionnelles mais souvent fortement conseillées dans le domaine de l'informatique, apportent elles aussi leur lot de problèmes. Automatiser la mise à jour du logiciel, des plugins, de Centreon, de Cacti et de la totalité des logiciels basés sur Nagios est difficile et couteux en temps. Enfin, l'interface nue du logiciel obligeant la configuration manuelle des fichiers de configurations (pouvant atteindre 20 000 lignes dans le cas du stage, plus pour un réseau plus important) est fastidieuse si on n'utilise pas une interface graphique proposée par Centreon par exemple.

[5] RR : Round-Robin, type de base de données suivant un algorithme d'ordonnancement spécifique

#### *3.1.2.2 Zabbix*

Autre solution open source, Zabbix est un logiciel qui met en avant sa simplicité d'installation, d'utilisation, et d'apprentissage. Contrairement à Nagios qui est un logiciel très lourd, Zabbix mise tout sur la légèreté en utilisant des agents de supervision[6] rapide et facile à installer. La base de données ici est de type MySQL[7] ce qui permets donc d'enregistrer autant d'information que l'on a d'espace disque disponible.

Le logiciel est découpé en trois grandes parties, un serveur qui gère le parc informatique, et envoie des alertes dans le cas de pannes. Un proxy[8] dans le cas de sites distants au serveur pour protéger les données transitant sur le réseau. Des agents pour récupérer les données des machines superviser et les renvoyer au serveur. Le tout est utilisé via une interface web propre au logiciel qui se veut facile d'utilisation.

Hélas, si la facilité d'utilisation de Zabbix est dans doute son plus grand point fort, le fait que le logiciel ait quelques inconvénients plus ou moins gênant peut exclure cette solution dans le choix d'un serveur de monitoring. En effet, le logiciel, contrairement à Nagios qui est très fragmenté, est un pack ou tout est compris, un avantage, mais aussi un défaut quand celui-ci n'intègre pas certaines fonctionnalités, puisqu'il n'est pas possible d'ajouter de plugins. De même, l'interface graphique étant épurée, elle manque de lisibilité sur certains écrans de contrôle, notamment celui des déclencheurs qui configurent l'envoi de mails lors de l'activation d'un événement (comme la panne d'un service).

[6] Agent de supervision : petit logiciel installé sur une machine à superviser qui la sonde et renvoie au serveur les valeurs relevées.
[7] MySQL : est un système de gestion de base de données optimisé pour la lecture des données
[8] Proxy : module logiciel destiné à présenter l'interface d'un composant ou d'un ensemble de composants logiciels afin de donner accès à leurs fonctionnalités

#### *3.1.2.3 FullAutomatedNagios / EyesOfNetwork*

FAN et EON propose plus ou moins le même service. Ce sont des distributions linux configuré pour proposer Nagios préinstallé. FAN propose directement les dernières versions de Nagios, Centreon, Nagvis et une multitude de plugins Nagios sur une distribution linux CentOS[9]. EyesOfNetwork lui propose aussi un tout en un en allant plus loin car il propose Cacti, GLPI et une interface spécialement conçu pour cette distribution facilitant la configuration des fichiers sous Nagios. L'avantage de ces deux solutions est bien entendu l'apport de tous les logiciels de supervision directement avec l'installation du système d'exploitation.

Les inconvénients de ce genre de solution est tout d'abord l'obligation d'installer un nouvel OS, l'OS est imposé et il faut donc s'adapter. Les mises à jour des logiciels de supervision sont difficiles à faire manuellement car ils ont été modifiés pour les distributions et il faut donc attendre une mise à jour de celle-ci pour tout mettre à jour. Les mêmes défauts que Nagios sont relevés étant donné qu'il est le logiciel de monitoring utilisé. Dans le cas d'EON, l'installation des modules complémentaires doit se faire après l'installation, et des problèmes de dépendances logicielles rendent leurs installations compliquées.

#### *3.1.2.4 Shinken*

Dernière solution envisagée, Shinken est un fork[10] du projet Nagios qui propose beaucoup de similitudes avec Nagios étant donné qu'il en est issu, mais bien entendu aussi certaines différences. Tout d'abord, à l'image de Nagios, les plugins respectant la syntaxe imposée sur les entrées sorties sont compatibles avec Shinken, ce qui rend l'application tout autant riche que Nagios. Cependant, une certaine ambigüité sur ce point apparait auprès des utilisateurs de Shinken, ce qui pourrait à terme poser des problèmes au fil des mises à jour. De même au niveau de la compatibilité avec les applications Centreon et autres logiciels axés autour de Nagios qui, dans la théorie,

[9] CentOS : Distribution Linux spécialisé serveur
[10] Fork : nouvelle branche de développement avec une optique différente

fonctionne avec Shinken, mais pourraient ne plus être compatibles après quelques nouvelles mises à jour.

L'avantage de Shinken sur Nagios vient de sa façon de traiter les données reçues. Shinken permet de découper une configuration en fragments et il est possible de ne traiter que certains de ces fragments, optimisant ainsi la supervision.

#### *3.1.2.5 Choix.*

Chaque application ou groupe d'application apporte son lot d'avantages et inconvénients. Déjà débarrassé des logiciels payants, choisir l'application libre la plus adaptée aux besoins de l'entreprise n'est pas facile, mais il a été décidé de prendre EyesOfNetwork qui réunissait en son sein tous les outils dont nous avions besoin dans le cadre du stage.

Bien que Shinken ait un nombre d'avantages, et que Zabbix soit de plus en plus plébiscité par la communauté du monitoring. EyesOfNetwork est la solution que nous avons choisie et mise en place pour superviser le réseau de SOFIA.

## 4. Fonctionnement de Nagios et d'EyesOfNetwork

Nagios est une application qui permet la surveillance d'un réseau informatique composé de serveurs, routeur, imprimantes et toutes autres machines ayant une adresse IP propre reliée à un réseau. Le programme est décomposé en trois parties. Le moteur de l'application qui s'occupe de l'ordonnancement des tâches et services à superviser. De multiples plugins qui complètent le système et permettent de superviser chaque ressource et services disponibles sur les ordinateurs surveillés. Et enfin une interface web qui affiche les données et autres informations souhaitées. Bien entendu, cette interface web peut être modifiée, comme dans le cas d'EON qui propose sa propre interface très largement inspirée de celle de Nagios.

Une fois le programme installée sur un serveur et correctement configuré, Nagios récupère les informations sur des services réseaux comme SMTP[11], HTTP[12] ou encore ICMP[13]. Il est possible de récupérer l'état de ressources systèmes comme la charge du processeur ou l'occupation des partitions des disques durs. La supervision de chacun des services se fait de façon simultanée et parallèle. Pour chaque service ou événement supervisé, Nagios vérifiera dans un certain laps de temps chacun d'eux. Si les messages de retour sont OK. Chacune des informations récupérée, et donc de leur état est ensuite visible dans des tableaux ou graphiques récapitulatif disponibles via l'interface Web de Nagios.

EyesOfNetwork se basant sur Nagios, propose une interface pour configurer celui-ci. Plusieurs outils contenus dans EyesOfNetwork permettent d'englober Nagios et le rende plus simple d'utilisation. EyesOfNetwork permettra ainsi des transitions entre les différents logiciels utilisés avec Nagios comme Cacti par exemple.

[11] SMTP : Simple Mail Transfer Protocol ou « Protocole simple de transfert de courrier » est le protocole lié aux messageries mails.
[12] HTTP : HyperText Transfert Protocol ou « Protocole de transfert hypertexte » est le protocole de communication client-serveur mis au point pour le World Wide Web.
[13] ICMP : Internet Control Message Protocol est l'un des principaux protocoles Internet. Il véhicule les messages d'erreur et de contrôle de la suite des protocoles Internet, notamment quand une machine est inaccessible

# 5. Installation et Configuration

## 5.1 Eléments à superviser et installation du serveur

Un tableau résumant les éléments à superviser est disponible en annexes de ce rapport. En résumé, il faut donc superviser sur toutes les machines, l'état même de la machine si elle est allumée, éteinte ou inaccessible du à une panne routeur, il faut aussi surveiller sur chacune d'elles, la mémoire, l'espace disque et la charge processeur. Enfin pour les serveurs, des vérifications sur l'activité de service devront être suivie de prêt.

Le serveur a dans un premier temps été installé sur une machine virtuelle puis transféré lors de la virtualisation des serveurs de SOFIA vers un serveur global. L'installation de Nagios a été automatique lors de l'installation de CentOS. Il a fallut installer en plus des modules optionnels en passant par une installation manuelle. Des problèmes de dépendances entre les modules imposaient des mises à jours non présente sur le DVD d'installation, ce qui a posé quelques problèmes de compatibilité pour que l'interface Web d'EyesOfNetwork reconnaisse chaque module, notamment GLPI pour la gestion du parc.

## 5.2 Configuration des machines clientes

### 5.2.1 Explications

Pour fonctionner correctement, il est nécessaire d'installer sur la totalité des machines à superviser le client SNMP[14]. Pour les machines fonctionnant sous linux, il suffit d'activer le démon [15] « SNMPD » avec une simple commande en mode administrateur. Dans le cadre du stage, seul un serveur fonctionnait sous linux, en plus du serveur de supervision, il a donc fallu activer le démon et configurer le client SNMP pour qu'il soit reconnu par Nagios. En effet, même activé, il est possible que Nagios ne puisse pas récupérer d'information de ses machines clientes. Il faut que celles-ci accepte l'adresse entrante du serveur, ainsi qu'un « nom de communauté » dans notre cas

[14] SNMP : protocole simple de gestion de réseau (Simple Network Management Protocol)
[15] Démon : processus lancé au démarrage de la machine

« EyesOfNetwork ». Ce nom de communauté est utile pour les requêtes SNMP et constitue une sécurité supplémentaire, le client SNMP ne répondant qu'à ce nom de communauté précis.

### 5.2.2 Installation par automatisation

Dans le cas des machines Windows, ce qui correspond donc à 98% du réseau excluant ainsi les machines sous Linux et le serveur AS/400, l'installation du client SNMP se fait soit à l'installation de Windows, soit en modifiant les paramètres de configuration. Dans certains cas, le client est installé mais désactivé. Dans d'autres cas il est nécessaire de l'installer via le CD/DVD d'installation. Plusieurs choix ce sont donc offerts à nous pour l'installation de cet élément crucial au fonctionnement du serveur. Nous avons dans un premier temps essayé de passer par le service de l'Active Directory[16] qui aurait permettre l'installation sur l'ensemble du parc informatique du client SNMP. Cependant, après plusieurs essais, il était difficile de mettre en œuvre cette solution. Le réseau étant composé de cinq versions de Windows différentes, le fichier d'installation du client SNMP est différent selon si Windows est une version 2000, XP ou version 64bits server 2003. Nous avons donc mis cette solution de côté pour l'installation du service, mais nous l'avons gardé pour la configuration de SNMP.

Pour configurer SNMP, nous sommes donc passés par l'Active Directory. Celui-ci permettant d'installer et de configurer l'ensemble d'un parc Windows, il a été possible de renseigner les arguments nécessaires au fonctionnement de SNMP. L'Active Directory a donc pu mettre en place le nom de communauté et l'adresse du serveur Nagios sur tous les postes Windows à l'exception des machines sous Windows 2000. Cette solution de configuration fonctionne même quand le service n'est pas installé. A l'installation du service SNMP, les éléments de sécurité seront directement configurés sans modifications de l'utilisateur.

[16] Active Directory : service Microsoft permettant d'appliquer des stratégies, d'installer des logiciels et d'installer des mises à jour.

### 5.2.3 Installation par télémaintenance

N'ayant pas pu installer automatiquement via l'Active Directory le client SNMP sur toutes les machines du parc informatique du réseau de SOFIA, il a donc fallu trouver d'autres solutions. On m'a donc proposé la solution de passer par le logiciel DameWare[17] pour installer sur des postes à distance sans avoir à immobiliser la machine. Le logiciel étant très complet, il propose d'installer un service en renseignant un fichier « .exe » et il l'installera ainsi sur la machine cible.

Un problème est cependant survenu avec cette méthode. Installant bien le service SNMP, il était impossible de le configurer. Des tests ont été réalisés sur plusieurs types de machines dont le Windows XP sur lequel je travaillais, et il était impossible d'accéder à l'onglet sécurité du client si l'installation était réalisée via DameWare. Enfin, une dernière tentative en essayant d'imposer la configuration via un fichier « .reg » contenant les informations nécessaires à Windows pour configurer correctement le service via le registre. Mais cette solution pouvait comporter des problèmes d'incompatibilités sur les ordinateurs distants. Cette solution a donc aussi été mis de côté.

### 5.2.4 Installation manuelle via logiciel de contrôle à distance.

Dernière solution pour installer le client SNMP sur toutes les machines et solution la plus longue à mettre en place, a été d'installer un à un le client SNMP sur chaque machine à superviser. Cette solution comportait deux problèmes. Premièrement, le temps, il y avait beaucoup de machines à superviser, et se connecter à chacune d'elles était long. Ensuite, il fallait immobiliser la machine le temps de faire l'installation. La majeur partie des ordinateurs supervisés étant des caisses de magasin, il a donc fallu mettre en place un système pour réduire le temps d'immobilisation le plus possible. Pour se faire, j'ai mis en place un script batch[18] afin de condenser les lignes de commandes à écrire dans le terminal du pc distant. De plus, l'installation du client SNMP ne peut se faire qu'en ayant les droits

[17] DameWare : Logiciel de télémaintenance permettant la maintenance à distance d'un poste.
[18] Script batch : script Windows exécutant des commandes le composant

d'administrateur, ce qui m'a forcé à rajouter une encapsulation de la commande d'installation dans une commande sécurisée permettant d'exécuter en administrateur. Une fois le script mis au point, je l'ai déposé sur l'un des serveurs accessible par tout le réseau.

Afin de ne pas perturber le travail des magasins, j'ai pris le contrôle de leur machine à des moments creux de la journée pour lancer mon script batch. L'installation se lançait donc rapidement et automatiquement sans aucune autre intervention demandant de valider une option ou de relancer la machine. Certaines machines demandaient par contre le CD d'installation de Windows, il a donc fallu que récupère la totalité des versions dématérialisées de Windows avec leur derniers Services Packs pour finaliser l'installation sur chacun des PC le demandant.

Enfin, seules les machines sous Windows 2000 demandaient une intervention supplémentaire car il fallait en plus configurer le client SNMP, l'Active Directory fonctionnement mal sous ces anciennes versions de Windows. Il m'a suffit d'aller renseigner les champs de l'onglet sécurité du service SNMP via la liste des services Windows.

## 5.3 Configuration de l'AS/400

Un Application System/400 est un serveur IBM avec une architecture différente des serveurs habituels. Fonctionnant avec un système d'exploitation qui lui est propre, sa configuration était donc assez différentes des autres serveurs. En effet, l'AS/400 ne propose pas d'interface graphique, uniquement des lignes de commandes. C'est à partir de ça que le serveur de monitoring pourra superviser ce serveur.

Il a fallu dans un premier temps, comme pour toutes machines, activer et configurer le client SNMP de l'AS/400. Initialement installé, il n'a eu besoin que de renseigner l'adresse du serveur Nagios et le nom de la communauté d'EyesOfNetwork. Cependant, c'est au niveau de la configuration via Lilac que l'AS/400 pose problème. De base, Nagios propose des plugins pour superviser des machines Windows, Linux voir Cisco ou d'autres machines assez rependues. Mais dans le cas de l'AS/400, Nagios ne proposait pas dans son « package » de base des plugins pour superviser la charge processeur ou l'espace disque utilisé sur le serveur.

Fort heureusement, un plugin développé par des membres de la communauté Nagios était disponible. Cependant, celui-ci n'était pas totalement fonctionnel pour l'AS/400 de SOFIA. L'AS/400 étant configuré en français, certains mots clé utilisés dans le plugin, vraisemblablement d'origine allemande, ne pouvait pas être reconnu. Dans ces conditions, le plugin ne pouvait pas communiquer avec l'AS/400.

Donc, dans un premier temps, après plusieurs essais pour repérer les mots clé à changer, le plugin, développé en Java, a du être ouvert pour y modifier des les mots resté en allemand, des termes comme « Jeton » ou « Option » étaient nécessaire au plugin pour se connecter à l'AS/400. Recompilé, il ne restait plus qu'à renseigner convenablement les options du plugin pour récupérer certaines données de l'AS/400.

## 5.4 Récupération de l'état de services sur les serveurs SOFIA.

Plusieurs serveurs étaient à superviser à SOFIA. En plus de récupérer l'état processeur, mémoire, et disque dur des machines, il fallait mettre en place une vérification de l'activation de plusieurs services sur certains d'entre eux. Ce que SNMP ne peut malheureusement pas faire.

Tout d'abord, il a fallut définir et reconfigurer un plugin de Nagios qui permets de sonder une machine pour savoir si un service est activé ou non. « check_nt » est utilisé avec un agent à installer sur les serveurs. A la manière de SNMP, ce plugin de Nagios à besoin d'un agent pour récupérer des informations sur les machines supervisées. Il a fallut installer NSClient++. Ce programme, lors de son installation, demande les adresses sécurisées, donc l'adresse du serveur, ainsi qu'un mot de passe. Le mot de passe, bien qu'optionnel sert à ce que la machine n'envoie pas les informations à un autre serveur que le serveur Nagios configuré pour ça.

Une fois les machines cibles configurées convenablement, il ne restait plus qu'à adapter Nagios pour qu'il affiche l'état des services voulus. Pour récupérer le nom des services, j'ai choisis de passer par DameWare qui affiche la liste des services de chaque machine rapidement. Une fois renseigné, Nagios peut donc afficher si le service est bien lancé, s'il est éteint ou s'il est dans un état inconnu.

## 5.5 Configuration des Templates

Nagios, ainsi que la plupart des programmes de supervision permettent la classification des machines par groupe nommé Templates. Le Template permet au serveur de supervision d'assigner à chaque machine qui en font partie, des commandes. Cela permet ensuite sous Nagios d'afficher des résultats unis. Pour mieux imager le rôle du Template, je vais donner un exemple concret de son utilisation sur les machines que j'ai du superviser.

Nous avons créé une multitude de Template remplaçant les Templates de base qui ne satisfaisaient finalement pas à l'utilisation que nous comptions faire de Nagios. Par exemple, un Template « Responsable_magasin » à pu regrouper la totalité des machines des

responsables des magasins. Etant souvent allumé et éteint, ces machines n'ont pas besoin de demander à Nagios d'envoyer un mail au superviseur chaque fois que la machine est allumée ou éteinte. On peut aussi sur ce même Template faire en sorte que les vérifications se fassent beaucoup moins souvent. L'objectif ici est donc de gagner en charge réseau et éviter des mails inutiles.

Un autre exemple de Template, est celui utilisé sur la totalité des machines. Comme il a été demandé ici de retourner, pour tout le réseau, la charge CPU, mémoire, et disque dur. J'ai donc configuré un Template

# 6. Finalisation du projet

## 6.1 Tests et ajustements

Les tests se sont déroulés en temps réels. Il n'y a pas eu de phase de test proprement dit, en effet, le serveur de supervision fonctionnant continuellement, ce qui permettait de vérifier constamment qu'il répondait bien aux données. Il était donc possible de vérifier constamment que le programme réagissait bien lorsque surgissait une panne.

Afin de tester l'afflux de mails envoyé par le serveur et éviter un débordement de la boite mail du superviseur. J'ai effectué quelques tests sur des périodes d'un jour. Avec un premier test à 1600 mails reçu en 24h, il était évident qu'il fallait réajuster les Templates pour en recevoir beaucoup moins. Les ajustements se sont fait via l'interface Lilac d'EyesOfNetwork en modifiant les Templates. De base, en utilisant les Templates de base, nous nous somme rapidement rendu compte que Nagios faisait des vérifications sur chaque machines avec un laps de temps très court. Donc une machine étant dans un état critique faisait émettre à Nagios un mail de notification, ce qui avait pour effet de remplir la messagerie du superviseur.

## 6.2 Gestion des imprévus et problèmes récurrents

Quelques imprévus, mais qui font aussi parties du métier, m'ont fait perdre beaucoup de temps dans la mise en place du serveur de supervision. Lié ou non à la virtualisation des serveurs du siège de SOFIA, une erreur au lancement du serveur rendait impossible son exécution et par mesure de sécurité par rapport aux données présentes sur le serveur, nous avons préféré attendre la fin de la journée que la virtualisation soit aboutie pour essayer de corriger l'erreur.

De même, un bug inexpliqué est survenu pendant ce stage sur le serveur venant perturber le serveur de supervision. Plusieurs éléments ont été touchés sans que l'on puisse expliquer comment c'est arrivé en vérifiant les logs.

Enfin lors de la configuration des fichiers de configuration de Nagios via l'interface Lilac, la moindre erreur ou le moindre oublie dans les options entrainaient des erreurs dans la mise à jour des fichiers. Ces erreurs ne pouvaient pas être corrigée via l'interface Lilac et obligeait donc d'ouvrir les fichiers de configurations très lourd et surtout entrecroisés. Par exemple, si une erreur dans la définition d'un service d'une machine était détectée, cela entrainait aussi une erreur dans la définition du fichier de configuration de la machine même. Les corrections étaient donc délicates car elles pouvaient entrainer d'autres erreurs. La solution mise en place face à ces problèmes récurrents, a été d'effacer totalement les blocs concernés dans les fichiers de configuration pour obtenir quelque chose de fonctionnel et de reconfigurer correctement sous Lilac jusqu'à ce que cela fonctionne.

# 7. L'application Web

## 7.1 Description de la tâche

En plus de la partie supervision, j'ai pu travailler très rapidement sur une ancienne application Web, afin de l'améliorer et d'effectuer un travail de correction de bug. L'application Web, utilisée sur l'intranet de la société est une application développée en PHP qui remonte des données comptables dans une base de données MySQL. Ma tâche était simple, apporter une solution à un problème d'affichage sur l'une page de l'application, et proposer un affichage formaté pour une impression sur feuille A4 de la page synthèse de l'application.

## 7.2 Contexte

Utilisé par les magasins franchisés Douglass de la société (les mêmes qui sont supervisés), l'application web permet d'enregistrer des données sur les ventes de chaque jour et de les enregistrer dans une base MySQL. L'application est composées de plusieurs pages ou il est possible de naviguer jusqu'à une page de synthèse récapitulant toutes les données entrées et proposant de valider pour enregistrer. De plus l'application web permet, d'enregistrer des informations sur des chèques différés déposé par les clients. L'interface Web propose donc d'enregistrer ses chèques et affiche de façon dynamique les chèques ajouté précédemment. Un problème a cependant été relevé lorsque le nombre de chèques affichés dépassait un certain nombre. Le bug n'empêchait pas l'application de fonctionner, mais pouvait amener à des erreurs dans le cas ou un chèque était ajouté deux fois.

## 7.3 Solutions apportées

Pour le bug de l'affichage, j'ai du reprendre entièrement la structure de donnée utilisée par le précédent code. Celui-ci utilisait de multiples tableaux imbriqués et utilisait une fonction de lecture progressive qui n'était pas adaptée à la structure du tableau trop complexe. J'ai donc recréé une nouvelle structure qui puisse s'adapter à la fonction de lecture et ainsi faire apparaitre le bon nombre de chèques sans pour autant modifier quoi que ce soit sur le fonctionnement de l'application.

Pour la demande du formatage de la feuille de synthèse pour l'impression, nous avons pu envisager plusieurs solutions, mais nous n'avons retenu que la solution de proposer un affichage sur une feuille PDF. En effet la feuille de synthèse récupère toutes les données enregistrées dans la base de données MySQL et les affiche sous forme de tableaux HTML qui peuvent dans certains cas s'imprimer sur plusieurs feuilles A4. Pour ne pas déformer l'affichage à l'écran, un bouton d'impression affichant une page PDF entièrement retravaillée a été implémenté et n'est accessible qu'une fois l'application finalisée. Un outil du nom de FPDF m'a permis de mettre en place cette solution.

D'autres petites fonctionnalités ont pu être ajoutées comme une redirection vers la page d'accueil de l'application, ou l'affichage de la date de la dernière utilisation de l'application. Ces modifications apportant surtout plus de confort et d'ergonomie.

## Synthèse du stage

Après une période de plusieurs jours d'essai, on a pu constater que le serveur en lui-même fonctionnait bien grâce à des retours par mails dès qu'un incident survient sur une machine. Le serveur répond aux principales exigences fixées au début du stage. Cependant, certains points auraient pu être améliorés et certains points n'ont pas pu être traités. La récupération de certaines données sur certaines machines du réseau n'ont rien données malgré des configurations qui semblaient correctes, aucunes données n'étaient retournées, donc je n'ai pas persisté dans cette voie. Il n'a pas été possible de satisfaire à la totalité des souhaits de l'entreprise. Je regrette aussi de ne pas avoir pu toucher à GLPI pour la gestion du parc réseau.

Ce stage m'a aussi permis de mettre en application mes connaissances accumulées durant mes trois années d'études, que ce soit en cours de réseaux ou de développement avec la modification d'un plugin développé par une équipe étrangère en langage JAVA ainsi qu'en PHP pour la modification et l'amélioration de l'application web. Bien entendu, j'ai aussi pu mettre en pratique des connaissances personnelles. J'ai pu affiner mes connaissances dans ces secteurs et voir même apprendre de nouvelles.

## Webographie

Liste des sites utilisés lors de ce stage, tous les liens ci-dessous ont été vérifié le 17 Juin 2011

http://www.eyesofnetwork.com/?lang=fr : site officiel d'EON

http://www.nagios.org/ : site officiel de Nagios

http://forum.eyesofnetwork.com/index.php : Forum d'aide d'EON

http://www.monitoring-fr.org/ : Site français sur la communauté du Monitoring

http://forum.centreon.com/ : Forum d'aide sur Centreon et Nagios

http://www.developpez.net/forums : Forum d'aide pour le développement pour le plugin AS/400

http://www.cacti.net/ : Site officiel du programme Cacti

## Bibliographie


Salima HAMMA

**Cours de réseaux informatiques (télécomm et réseaux)**

2011

Sébastien Cazalas

**Cours Informatique & Société de l'IUT de Nantes**

2010

Guillaume Ponçon , Libero Maesano

**Best practices PHP 5**

Edition Eyrolles

Jean Gabès

**Nagios 3 pour la supervision et la métrologie**

Edition Eyrolles

# Annexes

## I - Exemple de fichiers configuration de Nagios

```
define contactgroup{
        contactgroup_name       admins-ubuntu
        alias                   Administrateurs machines Ubuntu
        members                 ostaquet,david,manu
        }
```

```
define host{
        use                     generic-host
        host_name               fileserver
        alias                   Serveur fichiers
        address                 192.168.0.10
        check_command           check-host-alive
        }
```

```
define hostgroup{
        hostgroup_name  connectique
        alias           Routeurs, firewalls et gateway
        contact_groups  admins-router
        members         router
        }
```

```
define service{
        name                            generic-service
        active_checks_enabled           1
        passive_checks_enabled          1
        parallelize_check               1
        obsess_over_service             1
        check_freshness                 0
        notifications_enabled           1
        event_handler_enabled           1
        flap_detection_enabled          1
        process_perf_data               1
        retain_status_information       1
        retain_nonstatus_information    1
        is_volatile                     0
        check_period                    24x7
        normal_check_interval           5
        max_check_attempts              3
        retry_check_interval            1
        notification_interval           0
        notification_period             24x7
        notification_options            c,r
        register                        0
        }
```

```
define timeperiod{
        timeperiod_name service_open
        alias           Heures de service
        monday          07:00-22:00
        tuesday         07:00-22:00
        wednesday       07:00-22:00
        thursday        07:00-22:00
        saturday        07:00-22:00
        }
```

## II - Exemple de mail envoyé automatiquement par Nagios en cas de pannes

**Objet :** Services CRITICAL alert for Machine test/memory!

***** Nagios *****

Notification Type: PROBLEM

Service: memory
Host: Machine de test Quentin
Address: 192.168.1.170
State: CRITICAL

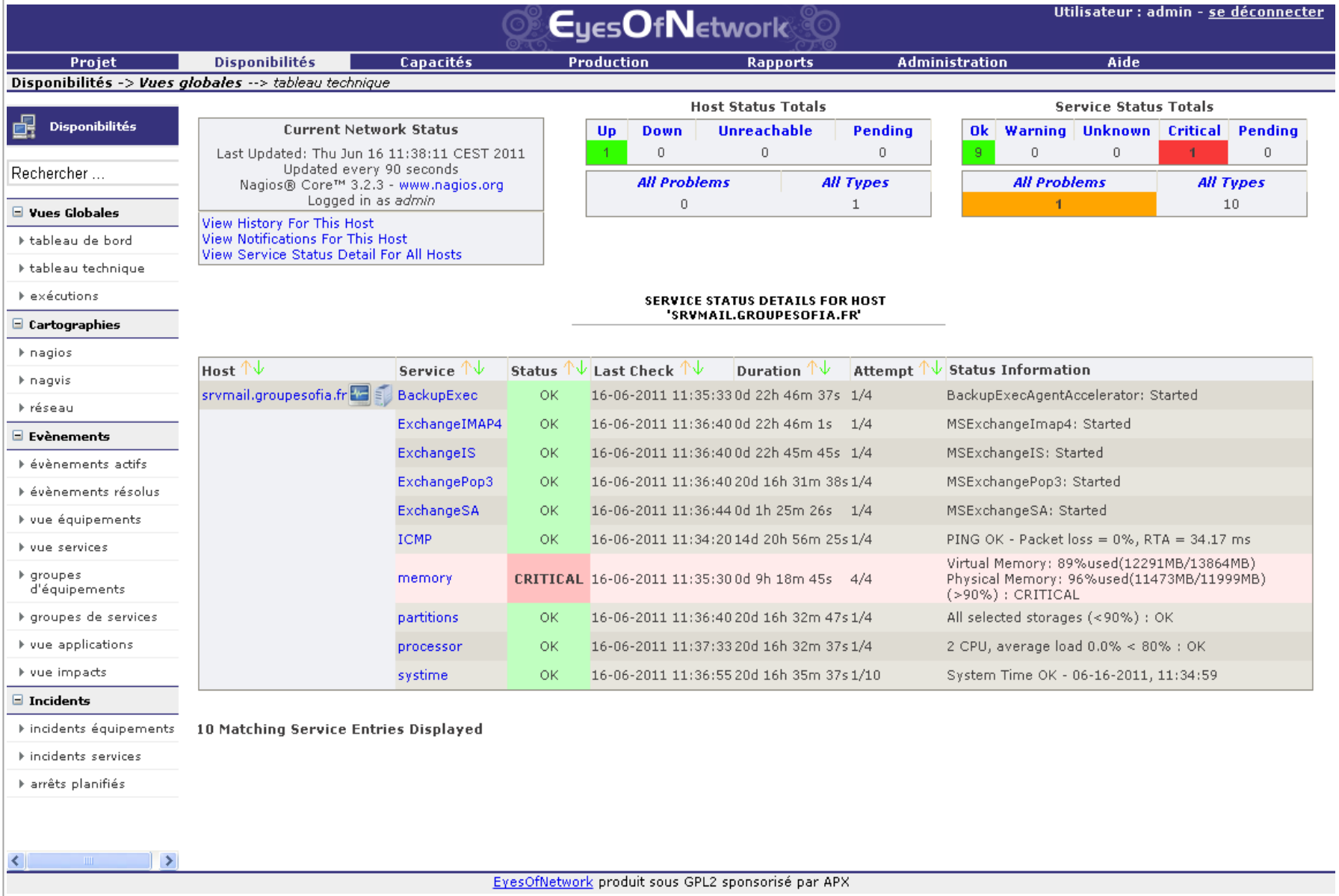
Date/Time: Fri Jun 10 15:23:00 CEST 2011

Additional Info:

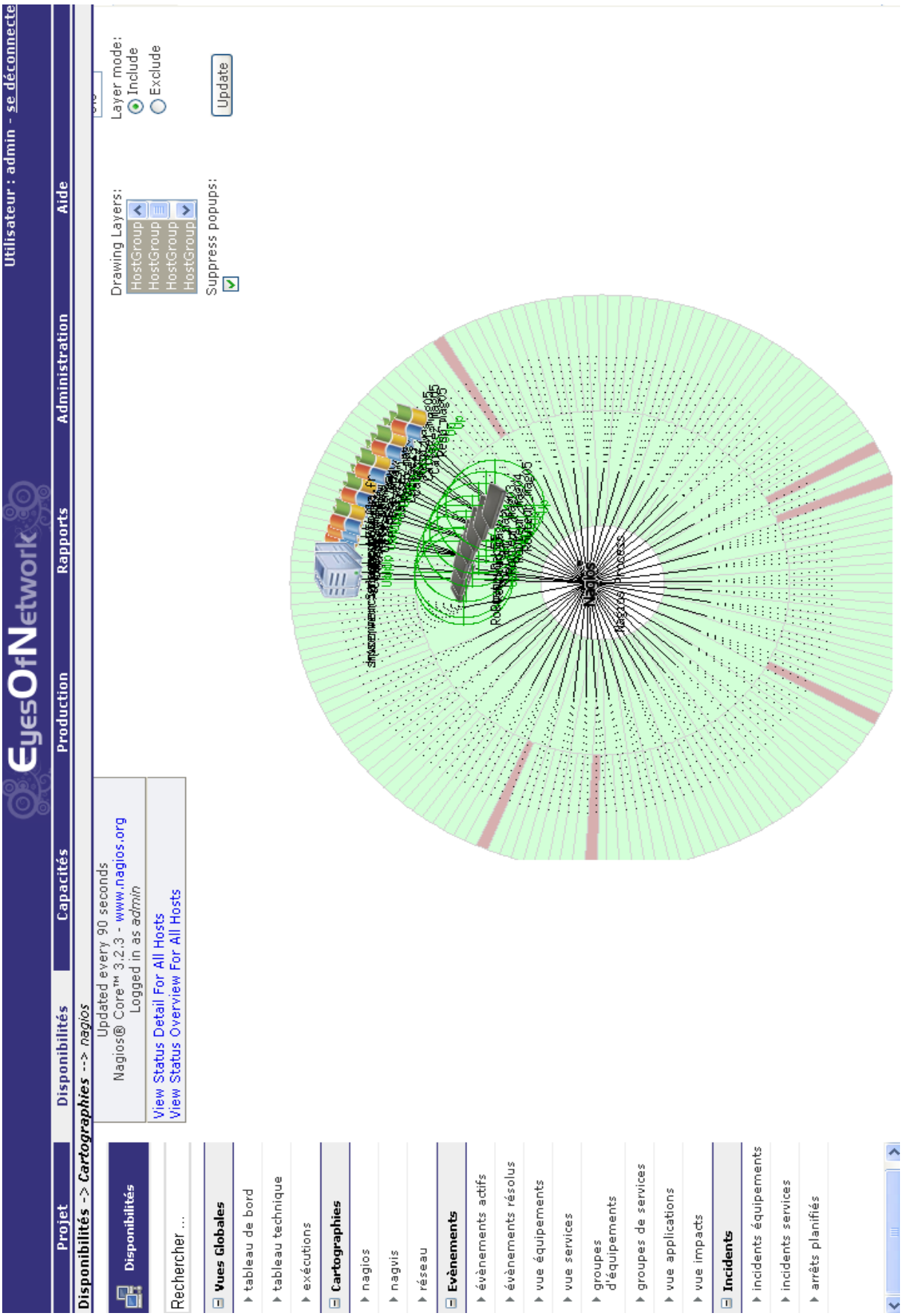
Physical Memory: 92%used(1887MB/2046MB)
Virtual Memory: 55% used(2171MB/3937MB) (90%) : CRITICAL

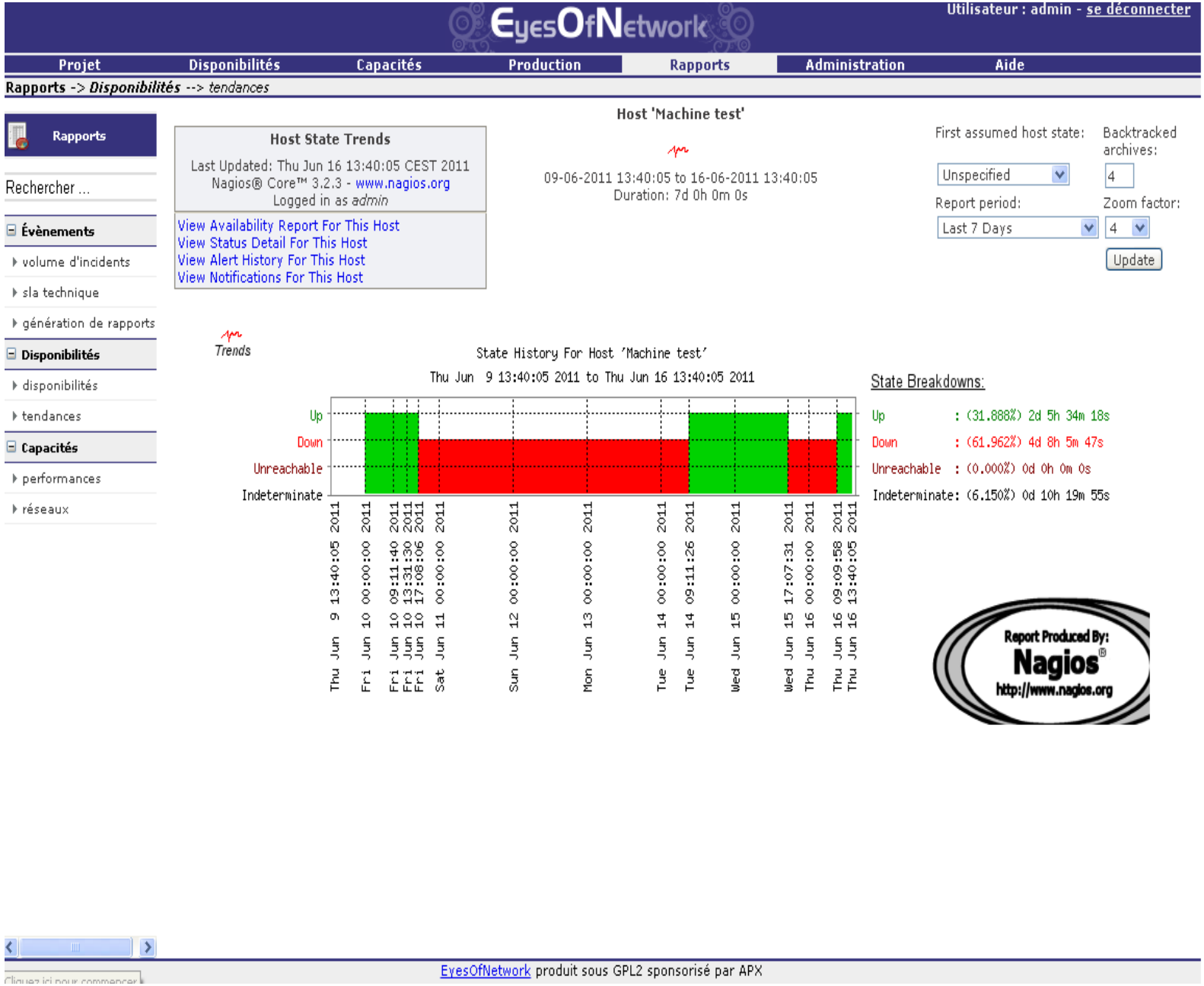
## III - Liste Supervision avec services à traiter

| Siege | Nom | @IP | A superviser commun | Spécifique |
|---|---|---|---|---|
| | AS400 | 192.168.1.1 | ICMP - CPU - Espace Disque - RAM | BackupExec |
| | Srvmail | 192.168.1.5 | ICMP - CPU - Espace Disque - RAM | Exchange - BackupExec |
| | Siege_web1 | 192.168.1.10 | ICMP - CPU - Espace Disque - RAM | Portail RH - BackupExec |
| | Siege_web2 | 192.168.1.11 | ICMP - CPU - Espace Disque - RAM | Oracle - BackupExec |
| | Srvblackberry | 192.168.1.12 | ICMP - CPU - Espace Disque - RAM | Blackberry - BackupExec |
| | Siegesec | 192.168.1.13 | ICMP - CPU - Espace Disque - RAM | BackupExec |
| | Intranet | 192.168.1.20 | ICMP - CPU - Espace Disque - RAM | HTTP |
| | Administration | 192.168.1.21 | ICMP - CPU - Espace Disque - RAM | |
| | Firewall | 192.168.1.253 | ICMP | |
| | Routeur_Siege | 192.168.1.254 | ICMP | |
| Playdis | | | | |
| | Routeur_Playdis | 172.16.150.1 | ICMP | |
| | Srv_Playdis | 172.16.150.200 | ICMP - CPU - Espace Disque - RAM | BackupExec |
| Loire Entrepot | | | | |
| | Routeur_LET | 172.16.200.1 | ICMP | |
| | Srv_LET | 172.16.200.200 | ICMP - CPU - Espace Disque - RAM | BackupExec |
| Clin d'Œil - Depot | | | | |
| | Routeur_Depot | 192.168.254.1 | ICMP | |
| | HPServeur | 192.168.254.3 | ICMP - CPU - Espace Disque - RAM | BackupExec |
| | Srvcommercial | 192.168.254.4 | ICMP - CPU - Espace Disque - RAM | BackupExec |
| Clin d'Œil - Magasins<br>xx correspond au numéro de magasin (sauf Quimper qui a le réseau 172.16.59.0) | | | | |
| | Routeur_magxx | 172.16.xx.1 | ICMP | |
| | Caisse1_magxx | 172.16.xx.2 | ICMP - CPU - Espace Disque - RAM | Vérification date |
| | Caisse2_magxx | 172.16.xx.3 | ICMP - CPU - Espace Disque - RAM | de fichier - Cron |
| | Caisse3_magxx | 172.16.xx.4 | ICMP - CPU - Espace Disque - RAM | |
| | Resp_magxx | 172.16.xx.10 | ICMP - CPU - Espace Disque - RAM | |


EyesOfNetwork
Utilisateur : admin - se déconnecter
Projet
Disponibilités
Capacités
Production
Rapports
Administration
Aide
Disponibilités -> Vues globales --> tableau technique
Disponibilités
Rechercher ...
Vues Globales
tableau de bord
tableau technique
exécutions
Cartographies
nagios
nagvis
réseau
Evènements
évènements actifs
évènements résolus
vue équipements
vue services
groupes d'équipements
groupes de services
vue applications
vue impacts
Incidents
incidents équipements
incidents services
arrêts planifiés
Current Network Status
Last Updated: Thu Jun 16 11:38:11 CEST 2011
Updated every 90 seconds
Nagios® Core™ 3.2.3 - www.nagios.org
Logged in as admin
View History For This Host
View Notifications For This Host
View Service Status Detail For All Hosts
Host Status Totals
Up Down Unreachable Pending
1 0 0 0
All Problems All Types
0 1
Service Status Totals
Ok Warning Unknown Critical Pending
9 0 0 1 0
All Problems All Types
1 10
SERVICE STATUS DETAILS FOR HOST 'SRVMAIL.GROUPESOFIA.FR'
Host Service Status Last Check Duration Attempt Status Information
srvmail.groupesofia.fr BackupExec OK 16-06-2011 11:35:33 0d 22h 46m 37s 1/4 BackupExecAgentAccelerator: Started
ExchangeIMAP4 OK 16-06-2011 11:36:40 0d 22h 46m 1s 1/4 MSExchangeImap4: Started
ExchangeIS OK 16-06-2011 11:36:40 0d 22h 45m 45s 1/4 MSExchangeIS: Started
ExchangePop3 OK 16-06-2011 11:36:40 20d 16h 31m 38s 1/4 MSExchangePop3: Started
ExchangeSA OK 16-06-2011 11:36:44 0d 1h 25m 26s 1/4 MSExchangeSA: Started
ICMP OK 16-06-2011 11:34:20 14d 20h 56m 25s 1/4 PING OK - Packet loss = 0%, RTA = 34.17 ms
memory CRITICAL 16-06-2011 11:35:30 0d 9h 18m 45s 4/4 Virtual Memory: 89%used(12291MB/13864MB) Physical Memory: 96%used(11473MB/11999MB) (>90%) : CRITICAL
partitions OK 16-06-2011 11:36:40 20d 16h 32m 47s 1/4 All selected storages (<90%) : OK
processor OK 16-06-2011 11:37:33 20d 16h 32m 37s 1/4 2 CPU, average load 0.0% < 80% : OK
systime OK 16-06-2011 11:36:55 20d 16h 35m 37s 1/10 System Time OK - 06-16-2011, 11:34:59
10 Matching Service Entries Displayed
EyesOfNetwork produit sous GPL2 sponsorisé par APX

## 2.Affichage de la cartographie automatique de Nagios




EyesOfNetwork
Utilisateur : admin - se déconnecter
Projet
Disponibilités
Capacités
Production
Rapports
Administration
Aide
Rapports -> Disponibilités --> tendances
Rapports
Rechercher ...
Évènements
volume d'incidents
sla technique
génération de rapports
Disponibilités
disponibilités
tendances
Capacités
performances
réseaux
Host State Trends
Last Updated: Thu Jun 16 13:40:05 CEST 2011
Nagios® Core™ 3.2.3 - www.nagios.org
Logged in as admin
View Availability Report For This Host
View Status Detail For This Host
View Alert History For This Host
View Notifications For This Host
Host 'Machine test'
09-06-2011 13:40:05 to 16-06-2011 13:40:05
Duration: 7d 0h 0m 0s
First assumed host state:
Unspecified
Backtracked archives:
4
Report period:
Last 7 Days
Zoom factor:
4
Update
Trends
State History For Host 'Machine test'
Thu Jun 9 13:40:05 2011 to Thu Jun 16 13:40:05 2011
Up
Down
Unreachable
Indeterminate
Thu Jun 9 13:40:05 2011
Fri Jun 10 00:00:00 2011
Fri Jun 10 09:11:40 2011
Fri Jun 10 13:31:30 2011
Fri Jun 10 17:08:06 2011
Sat Jun 11 00:00:00 2011
Sun Jun 12 00:00:00 2011
Mon Jun 13 00:00:00 2011
Tue Jun 14 00:00:00 2011
Tue Jun 14 09:11:26 2011
Wed Jun 15 00:00:00 2011
Wed Jun 15 17:07:31 2011
Thu Jun 16 00:00:00 2011
Thu Jun 16 09:09:58 2011
Thu Jun 16 13:40:05 2011
State Breakdowns:
Up : (31.888%) 2d 5h 34m 18s
Down : (61.962%) 4d 8h 5m 47s
Unreachable : (0.000%) 0d 0h 0m 0s
Indeterminate: (6.150%) 0d 10h 19m 55s
Report Produced By:
Nagios®
http://www.nagios.org
EyesOfNetwork produit sous GPL2 sponsorisé par APX

# V - Manuel d'utilisateur (procédure)

## Sommaire

1. Observer l'état du parc informatique ..... 41
1.1 Connexion application web ..... 41
1.2 Cartographie du parc ..... 41
1.3Vue globale réseau ..... 42
1.4 Vue globale de chaque sous-réseau / machine ..... 43
1.6 Courbes de tendance ..... 45
1.6.1 Rapport disponibilité des machines ..... 45
1.6.2 Rapport état des machines ..... 46

2. Mettre à jour le parc informatique sous Nagios. ..... 47
2.1 Lilac ..... 47
2.1.1 General ..... 47
2.1.2 Templates ..... 48
2.1.3 Network ..... 48
2.1.4 Tools ..... 48
2.2 Exporter les changements Lilac vers NAGIOS ..... 49
2.3 Configurer l'envoi des mails d'un Template ..... 50
2.4 Installation sur la machine à superviser ..... 51
2.4.1 Configuration surveillance performance ..... 51
2.4.2 Configuration surveillance services ..... 51

# 1. Observer l'état du parc informatique

## 1.1 Connexion application web

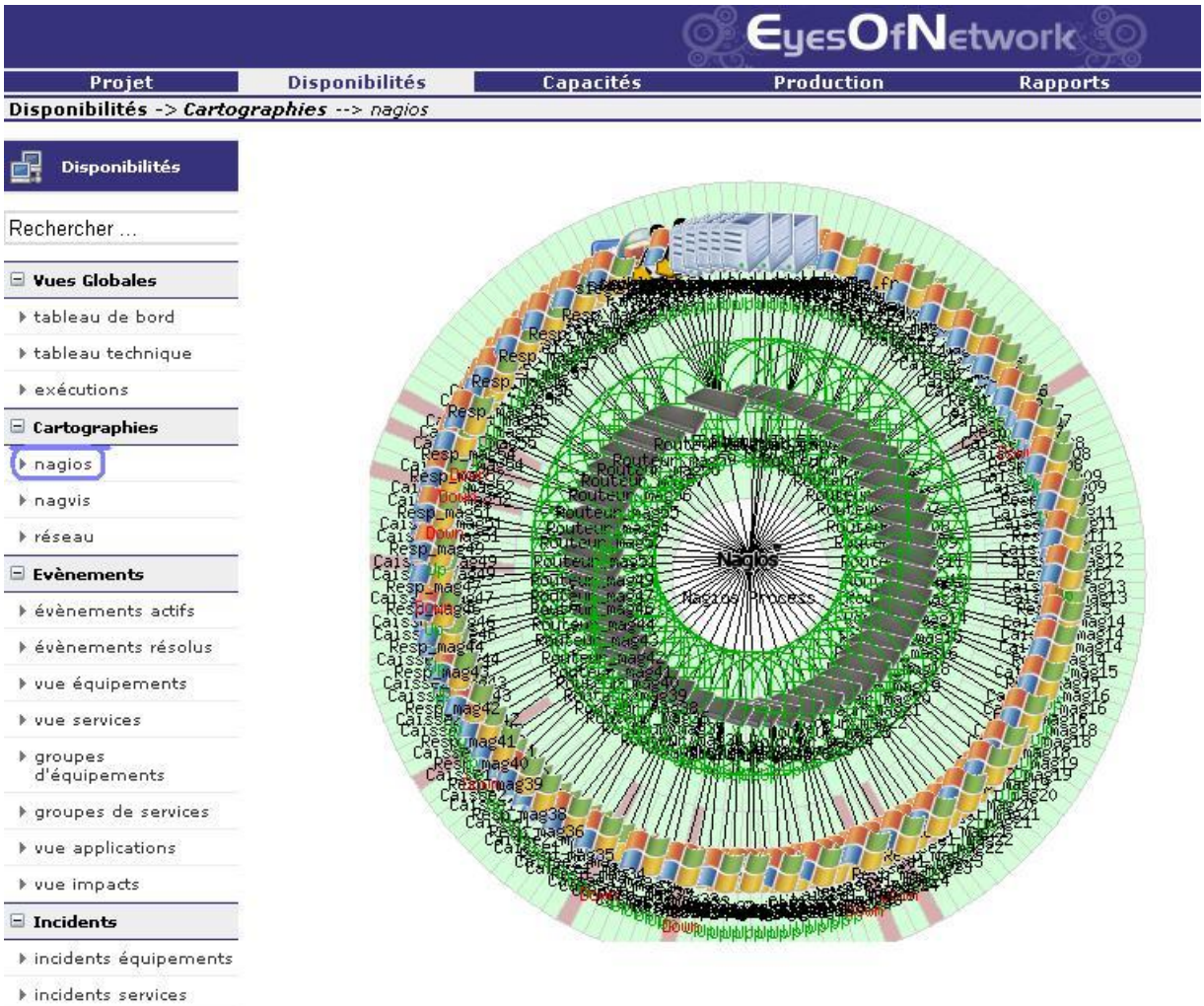
Le serveur EyesOfNetwork est accessible via un navigateur web via l'adresse serveur 192.168.1.21

| | |
|---|---|
| User : admin | MdP : ***** |

## 1.2 Cartographie du parc

Pour accéder à la vue en carte, dans le menu à gauche, sélectionnez **Nagios.**

Nagios créé automatiquement la carte qui est plutôt illisible, mais on peut voir d'un rapide coup d'œil si l'un des routeurs est *DOWN* car un cercle rouge apparaitra. Cette carte n'est utile que pour avoir un aperçu rapide de l'état du réseau.



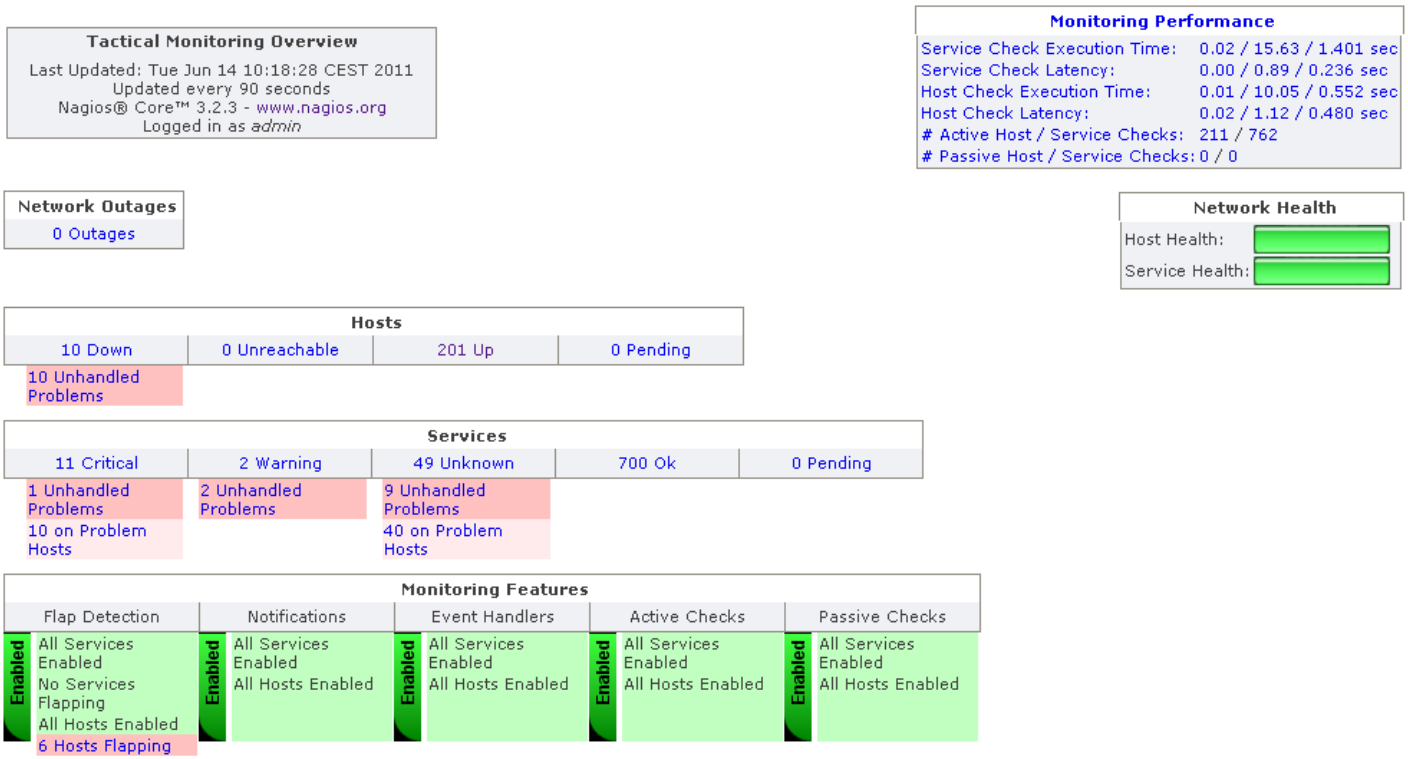
## 1.3Vue globale réseau

Il est possible d'avoir plusieurs aperçus du réseau en passante par **Disponibilité > Tableau technique**.

Cette page nous donne le résumé de l'état du réseau, ici 201 machines et équipements sont activés, 10 éteints, aucun injoignable, et aucun non plus dans un état d'attente.

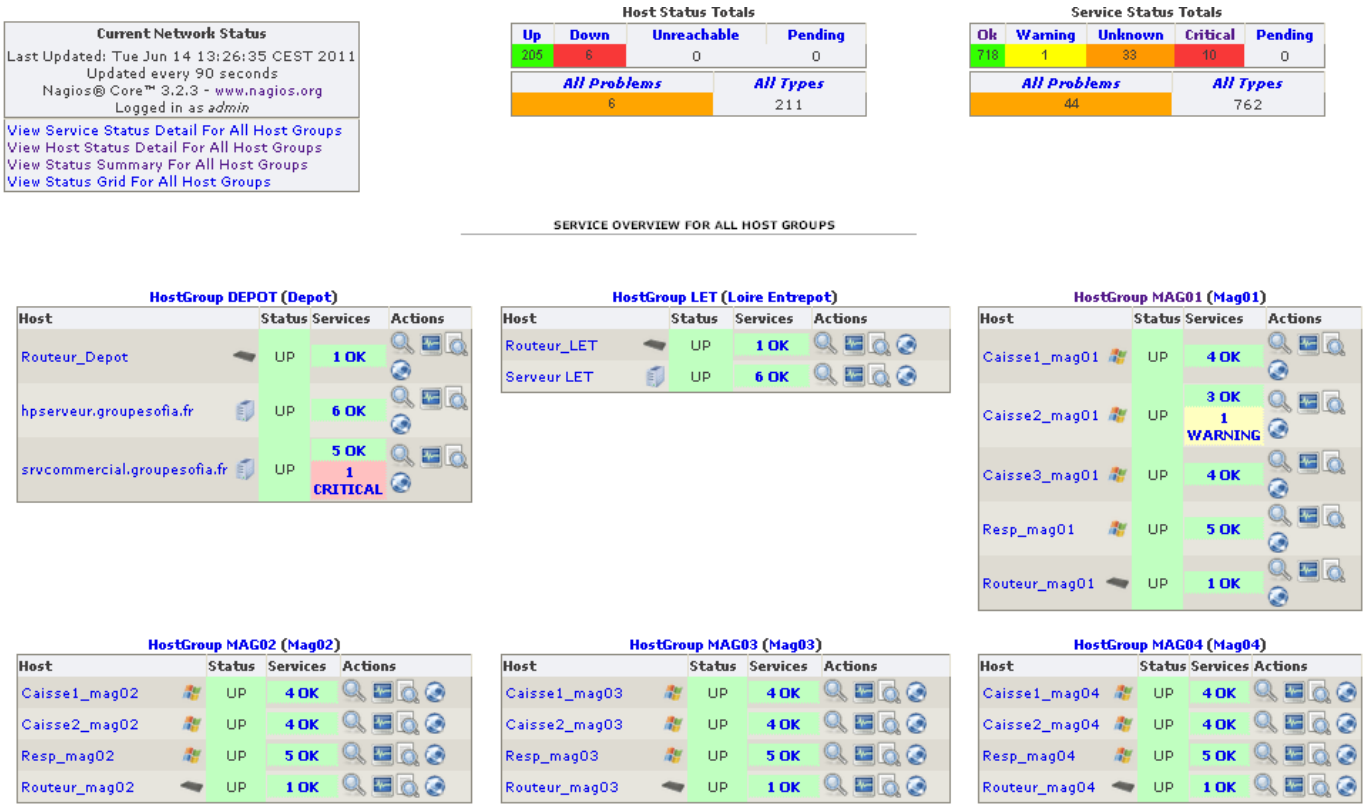
De même pour les services, c'est-à-dire chaque élément surveillé sur le parc informatique.

En cliquant sur le nombre d'hôtes dans l'état de son choix, il est possible d'avoir la liste des machines qui sont dans cet état. Par exemple, en cliquant sur « 10 Down » une liste de dix machines injoignables apparait.



## 1.4 Vue globale de chaque sous-réseau / machine

- Vue d'ensemble affichant l'état de tous les sous-réseaux :



Current Network Status
Last Updated: Tue Jun 14 13:26:35 CEST 2011
Updated every 90 seconds
Nagios® Core™ 3.2.3 - www.nagios.org
Logged in as admin

View Service Status Detail For All Host Groups
View Host Status Detail For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups

Host Status Totals

| Up | Down | Unreachable | Pending |
|---|---|---|---|
| 205 | 6 | 0 | 0 |

| All Problems | All Types |
|---|---|
| 6 | 211 |

Service Status Totals

| Ok | Warning | Unknown | Critical | Pending |
|---|---|---|---|---|
| 718 | 1 | 33 | 10 | 0 |

| All Problems | All Types |
|---|---|
| 44 | 762 |

SERVICE OVERVIEW FOR ALL HOST GROUPS

HostGroup DEPOT (Depot)

| Host | Status | Services | Actions |
|---|---|---|---|
| Routeur_Depot | UP | 1 OK | |
| hpserveur.groupesofia.fr | UP | 6 OK | |
| srvcommercial.groupesofia.fr | UP | 5 OK<br>1 CRITICAL | |

HostGroup LET (Loire Entrepot)

| Host | Status | Services | Actions |
|---|---|---|---|
| Routeur_LET | UP | 1 OK | |
| Serveur LET | UP | 6 OK | |

HostGroup MAG01 (Mag01)

| Host | Status | Services | Actions |
|---|---|---|---|
| Caisse1_mag01 | UP | 4 OK | |
| Caisse2_mag01 | UP | 3 OK<br>1 WARNING | |
| Caisse3_mag01 | UP | 4 OK | |
| Resp_mag01 | UP | 5 OK | |
| Routeur_mag01 | UP | 1 OK | |

HostGroup MAG02 (Mag02)

| Host | Status | Services | Actions |
|---|---|---|---|
| Caisse1_mag02 | UP | 4 OK | |
| Caisse2_mag02 | UP | 4 OK | |
| Resp_mag02 | UP | 5 OK | |
| Routeur_mag02 | UP | 1 OK | |

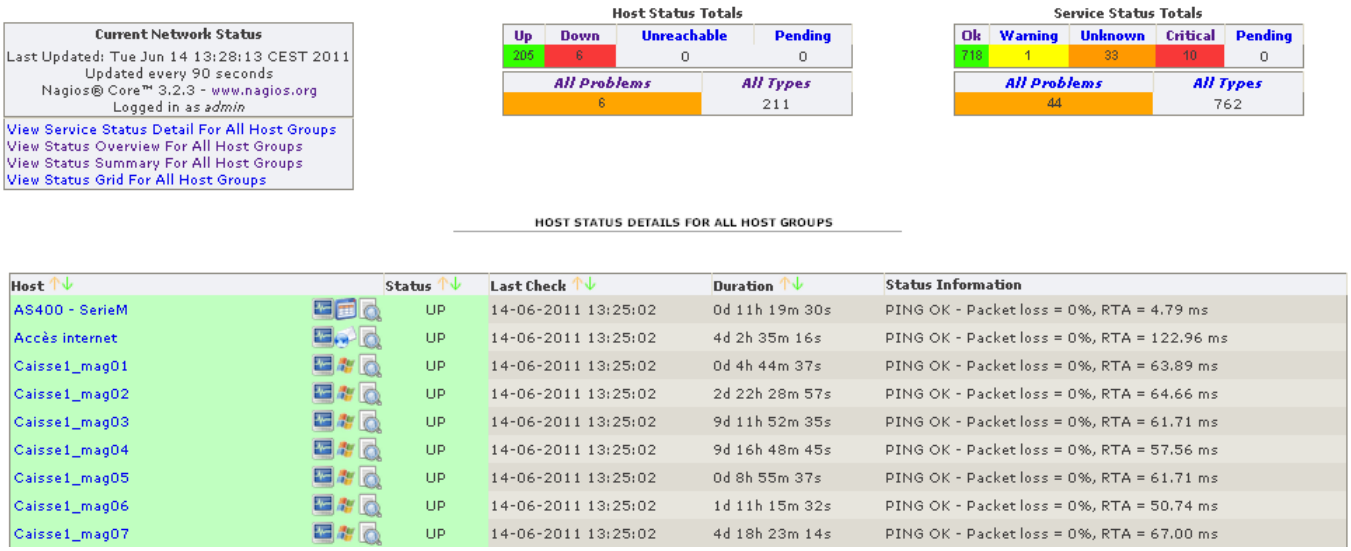
HostGroup MAG03 (Mag03)

| Host | Status | Services | Actions |
|---|---|---|---|
| Caisse1_mag03 | UP | 4 OK | |
| Caisse2_mag03 | UP | 4 OK | |
| Resp_mag03 | UP | 5 OK | |
| Routeur_mag03 | UP | 1 OK | |

HostGroup MAG04 (Mag04)

| Host | Status | Services | Actions |
|---|---|---|---|
| Caisse1_mag04 | UP | 4 OK | |
| Caisse2_mag04 | UP | 4 OK | |
| Resp_mag04 | UP | 5 OK | |
| Routeur_mag04 | UP | 1 OK | |

- Vue détaillée de toutes les machines du réseau :



Current Network Status
Last Updated: Tue Jun 14 13:28:13 CEST 2011
Updated every 90 seconds
Nagios® Core™ 3.2.3 - www.nagios.org
Logged in as admin

View Service Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups

Host Status Totals

| Up | Down | Unreachable | Pending |
|---|---|---|---|
| 205 | 6 | 0 | 0 |

| All Problems | All Types |
|---|---|
| 6 | 211 |

Service Status Totals

| Ok | Warning | Unknown | Critical | Pending |
|---|---|---|---|---|
| 718 | 1 | 33 | 10 | 0 |

| All Problems | All Types |
|---|---|
| 44 | 762 |

HOST STATUS DETAILS FOR ALL HOST GROUPS

| Host | Status | Last Check | Duration | Status Information |
|---|---|---|---|---|
| AS400 - SerieM | UP | 14-06-2011 13:25:02 | 0d 11h 19m 30s | PING OK - Packet loss = 0%, RTA = 4.79 ms |
| Accès internet | UP | 14-06-2011 13:25:02 | 4d 2h 35m 16s | PING OK - Packet loss = 0%, RTA = 122.96 ms |
| Caisse1_mag01 | UP | 14-06-2011 13:25:02 | 0d 4h 44m 37s | PING OK - Packet loss = 0%, RTA = 63.89 ms |
| Caisse1_mag02 | UP | 14-06-2011 13:25:02 | 2d 22h 28m 57s | PING OK - Packet loss = 0%, RTA = 64.66 ms |
| Caisse1_mag03 | UP | 14-06-2011 13:25:02 | 9d 11h 52m 35s | PING OK - Packet loss = 0%, RTA = 61.71 ms |
| Caisse1_mag04 | UP | 14-06-2011 13:25:02 | 9d 16h 48m 45s | PING OK - Packet loss = 0%, RTA = 57.56 ms |
| Caisse1_mag05 | UP | 14-06-2011 13:25:02 | 0d 8h 55m 37s | PING OK - Packet loss = 0%, RTA = 61.71 ms |
| Caisse1_mag06 | UP | 14-06-2011 13:25:02 | 1d 11h 15m 32s | PING OK - Packet loss = 0%, RTA = 50.74 ms |
| Caisse1_mag07 | UP | 14-06-2011 13:25:02 | 4d 18h 23m 14s | PING OK - Packet loss = 0%, RTA = 67.00 ms |

Pour accéder à ces vues, **Evénement > Vue équipement,** cliquer sur « View Status Overview For All Host Groups » pour arriver à la première capture d'écran. Chaque sous-réseau à été placé dans des groupes à part pour faciliter la visibilité.

Nagios fera donc apparaitre par tableau chaque sous groupe avec les services qui leur sont liés ainsi que leur état.

- L'état des machines :
  - **DOWN** signifie que la machine est éteinte ou inaccessible
  - **UNREACHABLE** signifie que le routeur est DOWN et que NAGIOS ne peut donc pas atteindre la machine
  - **UP**, tout fonctionne

- L'état des services :
  - **UP** : Le service est OK
  - **Warning** : Le premier seuil a été franchi, le service est à surveiller
  - **Critical** : Le second seuil est franchi, le service est dans un état critique, il faut intervenir.

Les services communs à chaque machine

- **ICMP** : une simple série de Ping, configurée pour en envoyer 4, au-delà, si aucune réponse de la machine, un WARNING ou un état DOWN sera affiché.
- **Partition** : NAGIOS vérifie l'état des partitions et donc du disque dur de chaque machine. Configuré pour envoyé un warning au-delà de 90% d'espace utilisé, un état CRITICAL au-delà de 95%.
- **Processeur** : de même, au-delà de 90% et 95 %, cependant, un état dit « flapping » permets d'éviter l'envoi de mail à chaque passage de la limite.
- **Mémoire** : affiche mémoire virtuelle et physique utilisée, et affiche aussi un état warning et critique en fonction de son utilisation

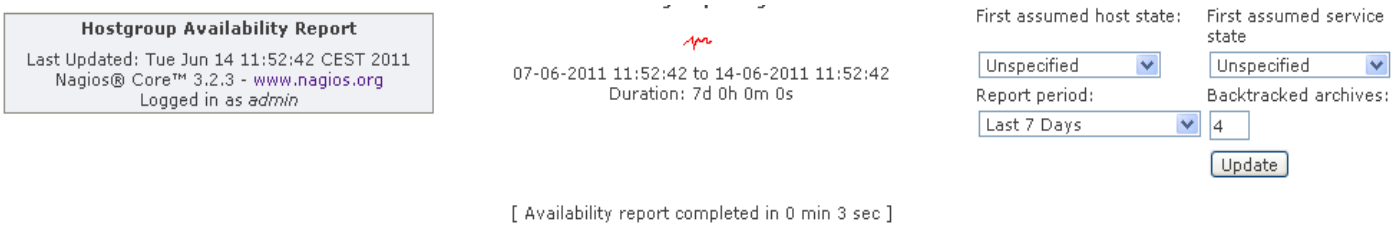
Les serveurs possèdent en plus des services supplémentaires, seul l'état actif ou éteint apparait.

## 1.6 Courbes de tendance.

Utile pour regarder si la machine a déjà eu des problèmes sur une période donnée, ou si c'est seulement ponctuel. Aller dans **rapport (menu en haut) > menu de gauche au choix**

### 1.6.1 Rapport disponibilité des machines

Pour obtenir un rapport sur l'état des différentes machines du réseau ou d'un sous réseau précis, dans Disponibilités choisir soit Host Group pour avoir une comme la capture d'image ci-dessous, mais pour un rapport plus détaillé, il faut choisir Host, et choisir la machine précise pour obtenir un rapport sur l'état des pannes, l'état des services et les entrées dans le journal sur la période choisie.



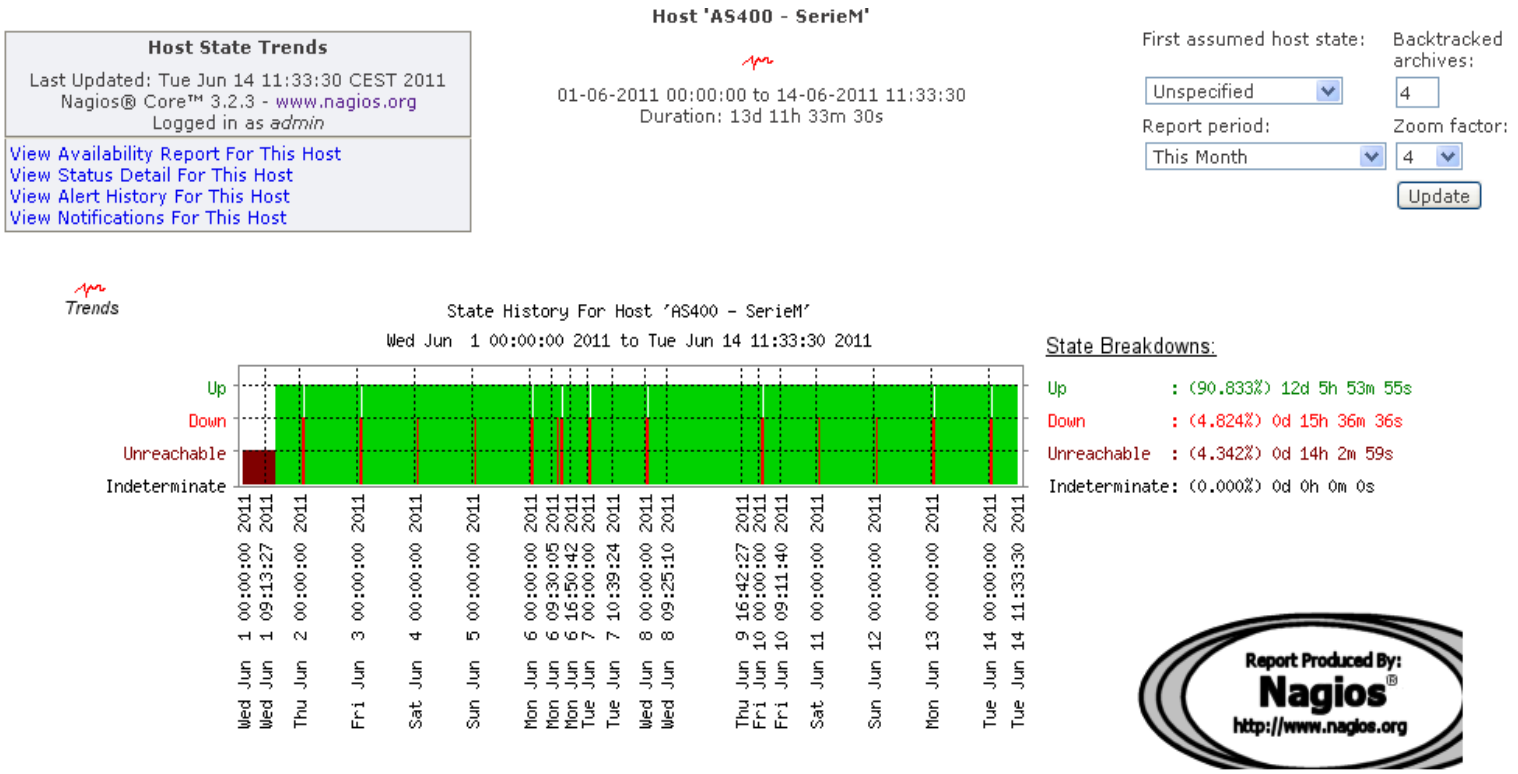

**Hostgroup 'Siege' Host State Breakdowns:**

| Host | % Time Up | % Time Down | % Time Unreachable | % Time Undetermined |
|---|---|---|---|---|
| AS400 - SerieM | 96.068% (96.068%) | 3.932% (3.932%) | 0.000% (0.000%) | 0.000% |
| Accès internet | 76.993% (76.993%) | 23.007% (23.007%) | 0.000% (0.000%) | 0.000% |
| Firewall | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% |
| Intranet | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% |
| Routeur_siege | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% |
| Supervision | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% |
| siege_web1.groupesofia.fr | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% |
| siege_web2.groupesofia.fr | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% |
| siegesec.groupesofia.fr | 78.874% (78.874%) | 21.126% (21.126%) | 0.000% (0.000%) | 0.000% |
| srvblackberry.groupesofia.fr | 96.486% (96.486%) | 3.514% (3.514%) | 0.000% (0.000%) | 0.000% |
| srvmail.groupesofia.fr | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% |
| Average | 95.311% (95.311%) | 4.689% (4.689%) | 0.000% (0.000%) | 0.000% |

### 1.6.2 Rapport état des machines

Il est possible d'obtenir un diagramme de l'état historique d'une machine. L'exemple si dessous concerne l'AS/400. Exécuté du 1er au 14 Juin, on peut observer son état dans le temps.

Pour cela, dans le menu de gauche, choisir « tendance » dans disponibilité puis Host, la machine à vérifier et spécifier les options de création du rapport.



# 2. Mettre à jour le parc informatique sous Nagios.

## 2.1 Lilac

Pour y accéder serveur 192.168.1.21 > **Administration (menu du haut) > Lilac (menu de gauche tout en bas)**

Nagios s'exécute en lisant certains fichiers de configurations, il est possible de les modifier manuellement mais une interface du nom de Lilac permet de les créer et modifier de façon automatique.
Lilac présente divers menus

General Templates Network Tools About

### 2.1.1 General

On y trouve tous les liens pour configurer Nagios, « Nagios Daemon Configuration », « Nagios Web Interface Configuration » et « Nagios Resources » sont déjà configuré convenablement, il n'y a plus de modifications à apporter.

Dans « Nagios Commands » on retrouve toutes les commandes qui tirent parties des plugins de Nagios, du ping à la vérification de l'état du processeur de l'AS/400. C'est ici qu'il faudra configurer une nouvelle commande s'il y a un nouveau plugin à rajouter.

« Time Periods » configure les plages horaires pendant lesquels Nagios envoie des mails. Le 24/7 envoie constamment des mails. Pour en configurer de nouvelles, il suffit de suivre la syntaxe suivante :

| | |
|---|---|
| Sunday | 00:00-24:00 |

Ainsi, il faut donc entrer le jour en anglais et la plage horaire.
« Contacts » et « Contact groups» configure les personnes à joindre par mail.
« Host group » permet l'affichage dans Nagios de groupes, cela créé une arborescence.

### 2.1.2 Templates

Il n'y normalement plus besoin de touche à la partie Templates. Dans le cas ou il y aurait des modifications à faire, il faut savoir que modifier un élément dans le template modifiera la configuration sur toutes les machines qui en hérite.

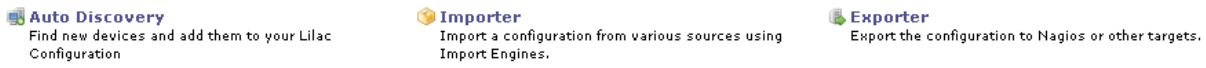
### 2.1.3 Network

L'onglet « Network » amène à la liste des machines du parc que traitera Nagios. Un outil « Nmap » pour rechercher des machines et les ajouter à cette liste existe en allant dans l'onglet « Tools » mais il est préférable de rajouter manuellement une machine s'il n'y en a pas beaucoup à rajouter via le lien « Add A New Child Host ».

Attention ---

Il faut configurer correctement la machine ajoutée, un oubli ou une erreur entrainera des erreurs ensuite l'hors de l'export. L'outil ne prévient pas l'utilisateur en cas d'oubli. Regarder comment les autres Templates ont été configurer et faire de même.

### 2.1.4 Tools


Auto Discovery
Find new devices and add them to your Lilac Configuration
Importer
Import a configuration from various sources using Import Engines.
Exporter
Export the configuration to Nagios or other targets.

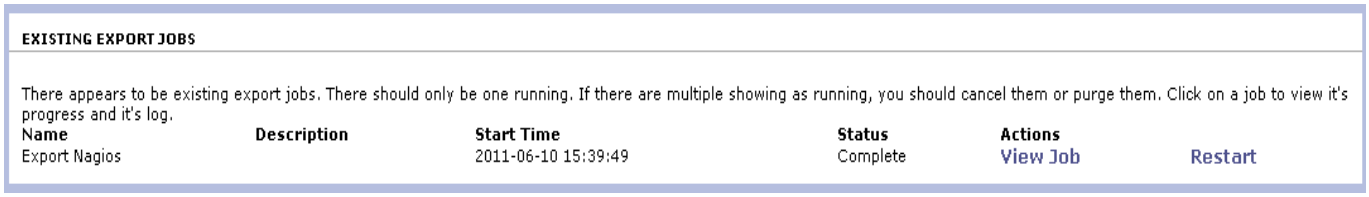
- Auto Discovery permet de rechercher des machines sur des plages d'IP et d'assigner un Template directement. Dans le cas ou il y a peu de machine, il est préférable de passer par l'outil « Add A New Child Host » dans Network.

- Importer ne sert que dans le cas d'un changement de serveur de supervision pour récupérer des fichiers de configurations déjà existants.

- Exporter est déjà configurer et est détaillé juste après.

## 2.2 Exporter les changements Lilac vers NAGIOS

Tout est déjà configurer, il n'y a plus rien à modifier, dans Tools > Exporter > ViewJob


EXISTING EXPORT JOBS
There appears to be existing export jobs. There should only be one running. If there are multiple showing as running, you should cancel them or purge them. Click on a job to view it's progress and it's log.
Name
Description
Start Time
Status
Actions
Export Nagios
2011-06-10 15:39:49
Complete
View Job
Restart

Et cliquer sur « Restart Job»

Si tout se passe bien ceci apparait.

JOB DETAILS
Job Name: Export Nagios
Job Id: 10
Start Time: 2011-06-14 10:58:55
Elapsed Time: 0 Hours 0 Minutes 17 Seconds
Current Status: Complete
Job Supplemental:
Backing Up Existing Configuration Files
Performing Preflight Check With Command: /srv/eyesofnetwork/nagios/bin/nagios -v /srv/eyesofnetwork/nagios/etc/nagios.cfg
Performing Nagios Restart With Command: /usr/bin/sudo /etc/init.d/nagios restart
Export Job Complete. Content Exported Successfully.
Restart Job | Remove Job | Return To Exporter

Sinon, dans le cas ou un oubli où une erreur a été faite un message d'erreur apparait.

Pour résoudre ce problème, inutile de retourner dans Lilac, ça ne sera pas pris en compte. Il faut aller modifier manuellement les fichiers concernés.

Pour cela, se connecter via vCenter au serveur de supervision

Rappel :

| |
|---|
| Login : supervision Mdp : ******* |
| Mdp root : ******* |

Ouvrir le terminal, mis en raccourcis dans la barre des tâches en haut.
Se mettre en administrateur via la commande :

```
sudo su
```

Un mot de passe est demandé : « ******* »

Et exécuter la commande suivante :

```
/srv/eyesofnetwork/nagios/bin/nagios -v /srv/eyesofnetwork/nagios/etc/nagios.cfg
```

C'est la commande qui permet d'exporter vers Nagios les fichiers de Lilac.
Un message d'erreur apparait et donne le nom du fichier endommagé et la ligne à modifier

L'idéal étant de supprimer complètement le bloc fautif et d'aller réparer l'erreur sur Lilac. En effet cela permet de recréer ce bloc de manière automatique et propre.
Un **`/etc/init.d/nagios restart`** est préférable après toute manipulation des fichiers.

Recommencer la procédure jusqu'à ce que ce soit bon, redémarrer le serveur manuellement si aucun changement n'apparait sur l'interface web.

## 2.3 Configurer l'envoi des mails d'un Template

- Changer le mail de la personne à prévenir.

**Lilac > Général > Contacts**

Cliquer sur admin ou créer un nouveau contact (qu'il faudra donc renseigner dans chacun des templates ou en tout cas ceux que l'on souhaite).
Puis Edit et changer l'adresse.

## 2.4 Installation sur la machine à superviser

### 2.4.1 Configuration surveillance performance

Pour chaque machine ajoutée au serveur de supervision, il faut installer le client SNMP sous Windows, ou l'activer sous Linux.

Sous Windows, il se trouve dans panneau de configuration > Ajout/Suppression de programmes > Composants Windows > SNMP

Si la machine fait partie du parc sous l'Active Directory, inutile de configurer la machine pour le serveur. Dans le cas contraire, ou pour les machines sous Windows 2000
**Exécuter > services.msc > ServiceSNMP > ClicDroit Propriété > Onglet Sécurité**

Communauté : EyesOfNetwork en Lecture Seule ou Lecture et Création
Serveur SNMP : 192.168.1.21

### 2.4.2 Configuration surveillance services

Pour surveiller un service précis, il faut installer NSClient++.
http://www.nsclient.org/nscp/downloads

Lors de l'installation, compléter le mot de passe : **** et l'adresse IP

Ensuite, **Lilac > Network > MachineASurveiller > Services > [Create A New Service For This Host] > Inheritance: generic_service > check [Edit], Check Command: check_nt > Check Command Parameters:**

$ARG1$: *****
$ARG2$: Nom_du_service, exemple "MSExchangeIS"